UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/696,584	10/24/2000	Ryuichi Iwamura	SONY-50P4042.US.P	3340

7590 04/22/2004

Wagner Murabito & Hao LLP
Two North Market Street
Third floor
San Jose, CA 95113

EXAMINER	
WU, ALLEN S	
ART UNIT	PAPER NUMBER
2135	2

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Reg

Office Action Summary	**Application No.** 09/696,584	**Applicant(s)** IWAMURA, RYUICHI	
	Examiner Allen S. Wu	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 October 2000* is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

KW

2. Claims 6, 14, 15, and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 recites the limitation "said received bitstream" in line 1 of claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 14 recites the limitation "said bitstream" in line 3 of claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 15 recites the limitation "the type" in line 1 of claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 24 recites the limitation "said broadcast hidden register" in line 3 of claim. There is insufficient antecedent basis for this limitation in the claim.

Drawings

3. New corrected drawings are required in this application because figs 3A-B and 7 are hand drawn and difficult to interpret. Furthermore, figures 2 and 8 contain

handwritten corrections that are hard to interpret (Host Computer System). Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

5. A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6.

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Dillon et al, US Patent 5,652,795.

As per claim 1, Dillon et al discloses processing a digital signal (see for example, abstract and col 3 ln 4-41) comprising: receiving an encrypted signal at a first logical circuit (see for example: frames are encrypted, col 3 ln 4-14 and col 4 ln 66-col 5 ln 2) determining a broadcast encryption key for said encrypted signal at a first location separate from said first logical circuit (see for example; data keys, col 6 ln 10-18) encrypting said broadcast encryption key (see for example, decrypt Data Keys, col 3 ln 56-60 and col 6 ln 10-20), transferring said encrypted broadcast encryption key over a communication link (see for example; satellite link, col 5 ln 3-16); at said first logical circuit (see for example Integrated Filter/Crypto Block, fig 2 and col 4 ln 61-col 5 ln 2), decrypting said encrypted broadcast encryption key to determine said broadcast encryption key (see for example, decrypting data key, col 5 ln 60-col 6 ln 19) at said first logical circuit, decrypting said encrypted signal using said broadcast encryption key (see for example col 6 ln 10-19).

8. Claims 10-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Mangold et al, US Patent 6,668,324.

As per claim 10, Mangold et al discloses generating a local encryption key (see for example, content encryption key, col 6 ln 31-39); transferring said local encryption key across a communication link to a first logical circuit (specific input device (see for example, key exchange col 6 ln 10-15 and col 6 ln 31-45) second logical circuit (see for example, decoding device, col 6 ln 31-45 and col 6 ln 54-64); with said local encryption key, encrypting said digital signal at said first logical circuit (see for example, col 6 ln 38-45); transferring said digital signal to said second logical circuit (see for example, col 6 ln 42-47); and using said local encryption key, decrypting said digital signal at said second logical circuit (see for example, col 6 ln 55-64), wherein said digital signal is transferred from said first logical circuit to said second logical circuit in an encrypted form (see for example col 6 ln 42-64).

As per claim 11, Mangold et al discloses the claimed limitations described above (see claim 10) and further discloses before transferring said local encryption key across said communication link, encrypting said local encryption key (see for example; col 6 ln 55-64).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2-4 and 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dillon et al, US Patent 5,652,795 in view of Searle, US Patent 6,683,954.

As per claim 2, Dillon et al discloses the claimed limitations as described above (see claim 1) and further discloses the step c1) accessing a value in a hidden register on said first logical circuit (see for example, UK Register, col 7 ln 11-25).

As for using said value accessed in step c1) for encrypting said broadcast encryption key, Dillon et al discloses encrypting the broadcast key with an encryption key inherently equal to the value in a register (see for example, col 5 ln 64-col 6 ln 19) since a DES algorithm is used (see for example, col 5 ln 1). DES algorithms are well known in the art to be form of symmetric encryption, wherein the same keys are use for both encryption and decryption. There must be a means of accessing such registers so that encryption with the proper values is performed. Searle discloses a method of encrypting a key with a value obtained from a client computer (see for example col 6 ln 62-col 7 ln 18). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Dillon et al because it would have increased key security by controlling the distributed use of the second key (see for example, Searle col 6 ln 28-31).

As for a value in a hidden register, the office takes official notice that hidden registers are notoriously well known in the art to provide for storing information unaccessible by software. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use hidden registers in storing values for encryption and decryption in system of Dillon because it would have increased security of tampering, by storing values in memory, which is harder to access.

As per claim 3, Dillon et al discloses the claimed limitations as described above (see claim 2) and further discloses modifying the value in said register (see for example; col 7 ln 60-col 8 ln 4). Since keys are stored in the registers, modification of the keys inherently modifies the registers storing the key values.

As per claim 4, Dillon et al discloses the claimed limitations as described above (see claim 1) and further discloses storing a value in a register on said first logical circuit (see for example; col 6 ln 46-col 7 ln 10). Dillon et al is silent on a host computer system performing encryption. However, Dillon et al discloses a digital signal that is encrypted with values in registers (see for example; col 5 ln 60-col 6 ln 9 and col 7 ln 11-21). One of ordinary skill in the art at the time of the applicant's invention would have realized that the encrypted digital signal must come from a source. Additionally, host computer systems are defined in the art as a system for providing data (digital signals). Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized a host computer system for encrypting such digital signals.

As for using said value accessed in a register for encrypting, Dillon et al discloses encrypting the broadcast key with an encryption key inherently equal to the value in a hidden register (see for example, col 5 ln 64-col 6 ln 19) since a DES algorithm is used (see for example, col 5 ln 1). DES algorithms are well known in the art to be form of symmetric encryption, wherein the same keys are used for both encryption and decryption. There must be a means of accessing such registers so that encryption with the proper values is performed. Searle discloses a method of encrypting a key with a value obtained from a client computer (see for example col 6 ln 62-col 7 ln 18). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Dillon et al because it would have increased key security by controlling the distributed use of the second key (see for example, Searle col 6 ln 28-31).

As for a value in a hidden register, the office takes official notice that hidden registers are notoriously well known in the art to provide for storing information unaccessible by software. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use hidden registers in storing values for encryption and decryption in system of Dillon because it would have increased security of tampering, by storing values in memory, which is harder to access.

As per claim 7, Dillon et al discloses the claimed limitations as described above (see claim 1) and further using values in registers to encrypt said broadcast encryption key (see for example, col 5 ln 64-col 6 ln 19 and col 6 ln 46-60). Dillon et al does not explicitly teach selecting a plurality of hidden registers on said first circuit to be used to encrypt said broadcast encryption key. Searle discloses a method of using a plurality of components to encrypt a broadcast encryption key (see for example; col 4 ln 59-col 5 ln 7). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Dillon et al because it would have increased key security by controlling the distributed use of the second key (see for example, Searle col 6 ln 28-31). Furthermore, in the Dillon-Searle combination, such components are used to define the key for encryption (see for example; Searle col 6 ln 28-31). Dillon et al further discloses indicating keys of encryption/decryption to the first logical unit (see for example; col 7 ln 36-50). Therefore, indicating the selection of hidden registers to said first logical circuit is inherent to the indication of keys in the teachings of Dillon et al.

As for a value in a hidden register, the office takes official notice that hidden registers are notoriously well known in the art to provide for storing information unaccessible by software. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use hidden registers in storing values for encryption and decryption in system of Dillon because it would have increased security of tampering, by storing values in memory, which is harder to access.

As per claim 8, Dillon et al discloses the claimed limitations as described above (see claim 1) and further using values in hidden registers to encrypt said broadcast encryption key (see for example, col 5 ln 64-col 6 ln 19 and col 6 ln 46-60). Dillon et al does not explicitly teach the use of a value in non-volatile memory for encrypting said broadcast encryption key. Searle discloses a method of client device dependent data to encrypt a broadcast encryption key (see for example; ROM, col 4 ln 59-col 5 ln 7). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Dillon et al because it would have increased key security by controlling the distributed use of the second key (see for example, Searle col 6 ln 28-31).

As per claim 9, Dillon-Searle discloses the claimed limitation as described above (see claim 8). Searle further discloses user dependent data in non-volatile memory (see for example; user name, col 4 ln 59-67).

11. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dillon et al, US Patent 5,652,795 in view of Nally et al, US Patent 5,808,629.

As per claim 5, Dillon et al discloses the claimed limitations as described above (see claim 1) and further discloses accessing a value in a register on said first logical circuit (see for example; col 7 ln 11-26) and using said value accessed, decrypting said encrypted broadcast encryption key (see for example, col 7 ln 27-35). Dillon et al does not explicitly teach the register being a hidden register. Nally et al discloses storing of data in hidden registers so that the data is inaccessible by software (see for example; col 14 ln 34-49). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nally et al within the system of Dillon because it would have increased security of tampering, by storing values in memory, which is harder to access.

12. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dillon et al, US Patent 5,652,795 in view of Blatter et al, US Patent 5,878,135

As per claim 6, Dillon et al discloses the claimed limitations as described above (see claim 1). Dillon does not explicitly teach the digital signal being compliant with the Motion Picture Experts Group (MPEG) format). Blatter et al discloses video protection of MPEG formatted data. MPEG format is a widely known standard in the art of video data formats. It would have been obvious to one of ordinary skill in the art to provide such digital video data format of Blatter et al within the system of Dillon et al because it would have increased security in the video data realm by extending such data and key protection to video data.

Digital data broadcast through a satellite link is well known in the art to include video data.

13. Claims 12-13 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Searle, US Patent 6,683,954.

As per claim 12, Mangold et al discloses the claimed limitations described above (see claim 11) and further discloses encrypting said local encryption key based upon a negotiated value (see for example; AKE, col 6 ln 9-15 and col 6 ln 35-38). Mangold et al does not explicitly teach encrypting said local encryption key based upon a value accessed in a register in said first logical circuit. Searle discloses a method of encrypting an encryption key based upon a value accessed in a system component (see for example, col 4 ln 59-col 5 ln 7). One of ordinary skill in the art at the time of the applicant's invention would have realized a register to be the similar to the listed components of Searle. Both Mangold et al and Searle disclose a method of key security and control in processing digital data. It would have been obvious to one of ordinary skill in the art to combine the teachings of Searle within the system of Mangold et al because it would have improved key integrity and control by using values accessed to by some system component as a key for encryption (see for example, Searle col 6 ln 28-31).

As per claim 13, Mangold et al discloses the claimed limitations described above (see claim 11) and further discloses encrypting said local encryption key based upon a negotiated value (see for example; AKE, col 6 ln 9-15 and col 6 ln 35-38). Mangold et al does not explicitly teach encrypting said local encryption key based upon a value accessed in a register in said second logical circuit. Searle discloses a method of encrypting an encryption key based upon a value accessed in a system component (see for example, col 4 ln 59-col 5 ln 7). One of ordinary skill in the art at the time of the applicant's invention would have realized a register to be the similar to the listed memory components of Searle. Both Mangold et al and Searle disclose a method of key security and control in processing digital data. It would have been obvious to one of ordinary skill in the art to combine the teachings of Searle within the system of Mangold et al because it would have improved key integrity and control by using values accessed to by some system component as a key for encryption (see for example, Searle col 6 ln 28-31).

As per claim 17, Mangold et al discloses the claimed limitations described above (see claim 10). Mangold et al does not explicitly teach polling a first hidden register in said first logical circuit. Searle discloses a means of polling memory (see for example, checksum is determined, col 8 ln 53-61), determining whether the value has been modified (see for example col 9 ln 6-17), and stopping said processing of said digital signal if said information was modified (see for example, col 9 ln 10-17). A hidden register is a form of memory used for storing data and is similar to the purposes of memory disclosed by Searle (see for example, ROM col 5 ln 1-7). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Mangold et al because it would have provided better security towards tamper-proofing by detecting whether memory storing valuable information is tampered or modified.

As per claim 18, Mangold-Searle discloses the claimed limitations described above (see claim 17). Searle further discloses notifying the user if information was modified (see for example; col 7 ln 61-col 8 ln 2). Communications with a broadcast provider is well known in the art. One of ordinary skill in the art at the time of the applicant's invention would have recognized that notification is sent by any communications means. In broadcasting, it is important for the provider to know such modification to important information to take appropriate measures. It would have been obvious to one of ordinary skill in the art to send such notification to a broadcast provider instead of a user because it would have provided important information to the party controlling the distribution of control.

14. Claims 19-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Searle, US Patent 6,683,954, and further in view of Nally et al, US Patent 5,808,629.

As per claim 19, Mangold et al discloses a first logical circuit (see for example, PCX module; col 6 ln 31-65 and 106 of fig 1) comprising a local encryptor (see for example; PCX encryptor, col 6 ln 31-42 and fig 4) and a second logical circuit (see for example; video decoder, col 6 ln 31-64) comprising a local decryptor (see for example; video decoder decrypts, col 6 ln 56-64), said local decryptor operable to decrypt a signal encrypted with said local encryptor (see for example, col 6 ln 31-64).

As for, the first logical circuit operable to decrypt a first local key using a first value stored in said first hidden register; and said second logical circuit operable to decrypt a second local key using a second value stored in said second hidden register, Mangold discloses a means of key exchange for obtaining such keys (see for example, col 6 ln 5-15 and ln 31-42). Mangold et al does not explicitly teach decrypting a local key using a value stored in a hidden register. Searle discloses a method of key security in processing digital data (see for example; abstract) including using a value stored in memory for decrypting an encryption key (see for example, col 4 ln 59-col 5 ln 7 and col 5 ln 65-col 6 ln 10). One of ordinary skill in the art at the time of the applicant's invention would have been able to replace the key exchange means of Mangold with the key encrypting and decrypting means of Searle within each respective first and second logical circuits. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Searle within the system of Mangold et al because it would have improved key integrity by controlling the distributed use of the second key (see for example, Searle col 2 ln 1-9 and col 6 ln 28-31).

Furthermore, the Mangold-Searle combination does not explicitly teach hidden registers. Nally et al discloses storing of data in hidden registers so that the data is inaccessible by software (see for example; col 14 ln 34-49). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nally et al within the Mangold-Searle combination because it would have increased security of tampering, by storing values in memory, which is harder to access.

As per claim 20, Mangold-Searle discloses the claimed limitations as described above (see claim 19). Mangold further discloses a host processor (see for example; CPU 115 fig 1); a communication link connecting said host processor to said first logical circuit and to said second logical circuit (see for example, bus 120 fig 1; processors or inherently connected to logical circuits through communication links in the setup of a computer); and memory coupled to said host processor (see for example, 108 of fig 1), said memory when run on said host processor are operable to generate a local key (see for example, session key, col 6 ln 42-55). In the Mangold-Searle combination, one of ordinary skill in the art at the time of the applicant's invention would have realized a first and second key for each of the logical circuits, since each key is generated from a value of the each circuit.

As per claim 21, Mangold-Searle discloses the claimed limitations as described above (see claim 20). Searle further discloses memory comprising instruction operable to access said value (see for example, computer implemented, col 6 ln 49-61). One of ordinary skill in the art at the time of the applicant's invention using hidden registers would have realized accessing the hidden register for accessing said value.

As per claim 22, Mangold-Searle discloses the claimed limitations as described above (see claim 19). Mangold et al furthest discloses a 1394 encryptor operable to encrypt signal for transfer over an IEEE 1394 communication link (see for example; DTCP fig 1 and col 4 ln 28-56).

As per claim 23, Mangold-Searle discloses the claimed limitations as described above (see claim 19). Mangold further discloses decrypting a broadcast signal (see for example, col 6 ln 16-30). As for decrypting an encrypted key using a value in said broadcast hidden register. Searle further discloses decrypting of an encrypted key using a value in stored memory (see for example; col 4 ln 59-col 5 ln 7 and col 5 ln 65-col 6 ln 10).

As for a broadcast decryptor comprising a broadcast hidden register and decrypting an encrypted key using a value in said broadcast hidden register. Mangold et al discloses a broadcast decryptor (see for example; DTCP decryptor, col 6 ln 10-15). Nally et al discloses storing of data in hidden registers so that the data is inaccessible by software (see for example; col 14 ln 34-49). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nally et al within the Mangold-Searle combination because it would have increased security of tampering, by storing values in memory, which is harder to access.

As per claim 24, Mangold-Searle discloses the claimed limitations as described above (see claim 22). Mangold further discloses memory when run on said host processor is operable to generate a broadcast encryption key (see for example; content key, col 6 ln 3-15). As for accessing a broadcast hidden register, and to encrypt said broadcast encryption key, Searle discloses means of accessing value in memory component (see for example; ROM, col 4 ln 59-col 5 ln 7) and encrypting a broadcast encryption key (see for example, col 5 ln 8-27). As for accessing said broadcast hidden register, Nally et al discloses storing of data in hidden registers so that the data is inaccessible by software (see for example; col 14 ln 34-49). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Nally et al within the Mangold-Searle combination because it would have increased security of tampering, by storing values in memory, which is harder to access.

15. Claim 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Blatter et al, US Patent 5,878,135.

As per claim 14, Mangold et al discloses the claimed limitations described above (see claim 10) and further discloses a header in said bitstream (see for example; col 6 ln 50-54). Mangold et al does not explicitly teach said first logical circuit to modify a header in said bitstream to indicate that said bitstream is encrypted. Blatter et al discloses a method of processing digital data (see for example; abstract) including a modifying a header in said bitstream to indicate that said bitstream is encrypted (see for example; encrypted indicator, col 3 ln 30-35). Both Mangold et al and Blatter et al disclose a method processing encrypted digital streams. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Mangold within the system of Blatter et al because it would have provided the option of processing non-encrypted data and encrypted data in the same system. Encrypting data is essential in security of important data, however, different security levels exists where certain data can be transferred in an unencrypted manner. A means for a system in determining such encrypted and unencrypted data is necessary to provide different security level approaches.

16. Claim 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Blatter et al, US Patent 5,878,135, as applied to claim 14 above, and further in view of Eyer et al, US Patent 5,485,577.

As per claim 15, Mangold-Blatter discloses the claimed limitations described above (see claim 14). The Blatter et al further discloses a command indicating a type of encryption (see for example; col 5 ln 35-54). Mangold-Blatter does not explicitly teach wherein said type is between even and odd encryption. Eyer et al discloses processing digital data (see for example; fig 1) comprising of switching between even and odd encryption (see for example col 8 ln 12-29). Mangold et al further discloses changing encryption keys (see for example; randomly generated content key, col 6 ln 39-42). Eyer et al discloses the even/odd encryption type as a means of changing encryption keys (see for example, col 7 ln 46-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Eyer within Mangold-Blatter because it would have provided an organized method of controlling encryption keys while maintaining the security of changing encryption keys.

17. Claim16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Eyer et al, US Patent 5,485,577.

As per claim 16, Mangold discloses the claimed limitations described above (see claim 10). Mangold does not explicitly teach, wherein said encryption key is switched between even and odd. Eyer et al discloses processing digital data (see for example; fig 1) comprising of switching between even and odd encryption (see for example col 8 ln 12-29). Mangold et al further discloses changing encryption keys (see for example; randomly generated content key, col 6 ln 39-42). Eyer et al discloses the even/odd encryption type as a means of changing encryption keys (see for example, col 7 ln 46-58). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Eyer within Mangold because it would have provided an organized method of controlling encryption keys while maintaining the security of changing encryption keys.

18. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mangold et al, US Patent 6,668,324, in view of Searle, US Patent 6,683,954 as applied to claim 19 above, and further in view of Eyer et al, US Patent 5,485,577.

As per claim 25, Mangold-Searle discloses the claimed limitations as described above (see claim 19). Mangold-Searle does not explicitly teach a plurality of hidden registers and a control register operable to store a value to indicate which of said hidden registers is used for encryption. Mangold discloses a means of changing keys (see for example; randomly generated, col 6 ln 40-42). Eyer discloses a first logical circuit (see for example; col 4 ln 29-47) including a plurality of memory banks (see for example; fig 4a and col 7 ln 59-65) and a control message (see for example; rekey message col 8 ln 1-11) for controlling which of said memory banks is used for encryption (see for example; col 8 ln 1-42). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Eyer within the Mangold-Searle combination because it would have increased key integrity and provided key organization through controlling which key is to be used for encryption.

As for a plurality of hidden registers and a control register, The office takes official notice that hidden registers are notoriously well known in the art to provide for storing information unaccessible by software. Searle further discloses values from memory to perform encryption and decryption of a local key as described above. Furthermore, control registers are well known in the art to operate in the same manner as a control message. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use hidden registers in storing values for encryption and decryption in the Mangold-Searle combination because it would have increased security of tampering, by storing values in memory, which is harder to access.

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent 5,805,706 discloses a method of encrypting data between a first and second logical device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW

[illegible]
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100